(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 024 626 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.08.2000 Bulletin 2000/31

(51) Int Cl.[7]: **H04L 9/08**, H04L 29/06

(21) Application number: **99101457.2**

(22) Date of filing: **27.01.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **International Business Machines Corporation**
Armonk, NY 10504 (US)

(72) Inventors:
- **Hermann, Reto**
  8863 Buttikon (CH)
- **Huseman, Dirk**
  8134 Adliswil (CH)

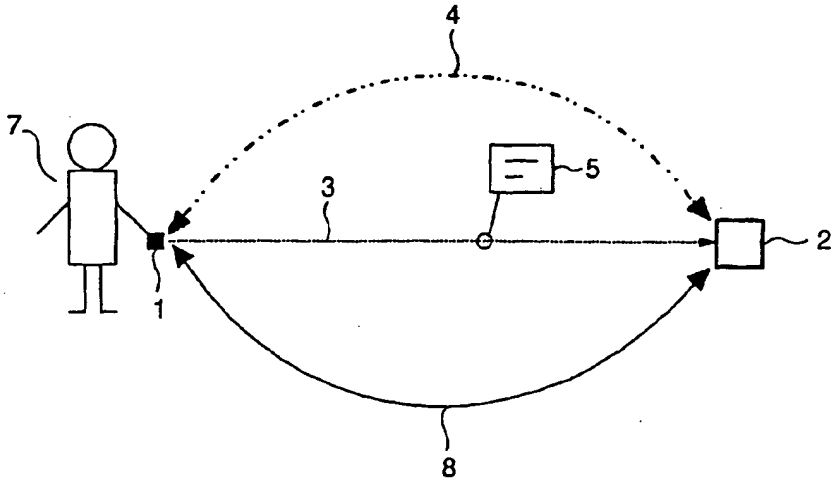
(74) Representative: **Heusch, Christian et al**
International Business Machines Corporation,
Säumerstrasse 4
8803 Rüschlikon (CH)

Remarks:
Amended claims in accordance with Rule 86 (2) EPC.

(54) Method, apparatus, and communication system for exchange of information in pervasive environments

(57) The present invention provides a method, an apparatus, and a communication system for the exchange of information in a networked pervasive environment. Therewith an authenticated and secure session can be achieved. Therefor are used a first device and at least a remote second device. A unidirectional wireless communication channel between the first device and the remote second device is initiated, whereby a sequence via the unidirectional wireless communication channel from the first device to the remote second device is sent in order to furnish the remote second device with encryption information. An encrypted response is sent via a wireless broadcast medium to the first device by using said encryption information for encryption.

Fig. 1



EP 1 024 626 A1

[0008] Xerox Corporation has developed a handheld computing device called PARC TAB. The PARC TAB is portable yet connected to the office workstation through base stations which have known locations. The PARC TAB base stations are placed around the building, and wired into a fixed wired network. The PARC TAB system uses a preset knowledge of the building layout and the identifiers of the various base stations to decide where it is by the strongest base station signal. A PARC TAB portable device has a wireless interface to the base stations. The PARC TAB system assumes that the PARC TAB portable device is always connected to the network infrastructure. The location of each portable PARC TAB device is always known to the system software.

[0009] The base stations establish regions and are connected to power supplies. PARC TAB communication systems have a star topology.

[0010] In an attempt to standardize data communication between disparate PC devices several companies, including Ericsson, IBM, Intel, Nokia, and Toshiba established the Bluetooth consortium to create a global standard for wireless RF-based connectivity between fixed, portable and mobile devices. There are many other adopter companies. The proposed standard comprises an architecture and protocol specifications ranging from the physical layer up to the application layer. The technology will for instance enable solutions to automatically synchronize application information kept in mobile devices with the similar information kept in a fixed desktop computer when users enter their offices. Enabling seamless voice and data transmission via wireless, short-range radio, the Bluetooth technology will allow users to connect a wide range of devices easily and quickly, without the need for cables, expanding communications capabilities for mobile computers, mobile phones and other mobile devices. The Bluetooth operating environment is not yet fully defined, but there are expected to be similarities with the IrDA (Infrared Data Association) specification and the Advanced Infrared (Air) specification. Other aspects that probably will find their way into Bluetooth might stem from the IEEE standard 802.11 and/or HIPERLAN, as promulgated by the European Telecommunications Standards Institute (ETSI).

[0011] Bluetooth radio technology provides a mechanism to form small private ad-hoc groupings of connected devices away from fixed network infrastructures. Bluetooth makes a distinction between a master unit - which is a device whose clock and hopping sequence are used to synchronize all other devices - and slave units in the same network segment. In other words, the Bluetooth approach is centralized. A query-based discovery scheme is used for finding Bluetooth devices with an unknown address. Queries are also centralized at a registry server. It is a drawback of such a centralized approach that there is a central point of failure. It is another disadvantage of such a system that more overhead is required than in a distributed scheme. The main problem of such a system is in locating a single registry server, and what to do if it disappears. If a random two devices encounter each other they must first recognize each other's presence, then decide which is the registry server, and then go about their business of communicating. It is this continual selection and re-selection of a leader that causes the increased overhead. The alternative is to expect users to carry one device that they always have with them, and make it always the leader. This, however, is not always a practical option.

[0012] The Infrared Data Association (IrDA) is an association of over 150 companies world wide focused on providing infrared standards and specifications to ensure the quality and interoperability of the infrared technology. IrDA-D is the infrared data transmission standard designed for data transfer over a distance of 1 m, scaleable from 115 kb/s to 4Mb/s or 16 Mb/s in the near future. There is a wide range of supported hardware and software platforms. IrDA Data defines a standard for an interoperable universal two way cordless infrared light transmission data port and is recommended for high speed short range, line-of-sight, point-to-point cordless data transfer. IrDA Data Protocols consist of a set of mandatory protocols and optional protocols. However, the original specifications show some drawbacks and restrict the data communication such that only one pair of devices could communicate in the same infrared space at one time. In a collaboration between the companies Hewlett-Packard and IBM a further specification, called the Advanced Infrared (Air), has been developed which will define the next generation of infrared data communication systems. Air is proposed for in room multipoint to multipoint connectivity. The distance and data rate are variable ranging from 250 kb/s over 8 m to 4 Mb/s over 4 m. It is designed for cordless connections to multiple peripherals and meeting room collaboration applications. More details about IrDA can be found at the IrDA web site http://www.irda.org.

[0013] HomeRF (based on Shared Wireless Access Protocol (SWAP) is another example of an operating environment which can be used to connect devices. A HomeRF Working Group was formed to provide the foundation for a broad range of interoperable consumer devices by establishing an open industry specification for wireless digital communication between PCs and consumer electronic devices anywhere in and around the home. The working group, which includes the leading companies from the personal computer, consumer electronics, peripherals, communications, software, and semiconductor industries, is developing a specification for wireless communications in the home called the SWAP. The HomeRF SWAP system is designed to carry both voice and data traffic and to interoperate with the Public Switched Telephone Network (PSTN) and the Internet; it operates in the 2400 MHz band and uses a digital frequency hopping spread spectrum radio. The SWAP technology was derived from extensions of existing cordless telephone (DECT) and wireless LAN

cation partner. People are accustomed to pointing to things from their childhood on. Additionally, pointing has the advantage of explicitly selecting a communication target: e.g. with PAN links the user has to actually touch the communication target; with laser links a communication partner can be selected visually.

[0025] If the two devices share the same wireless broadcast medium and are part of a local network then the advantage occurs, that an initiated session can be continued even if the user with the personal device changes his location by walking to other rooms or floors. This will be helpful if the personal device downloads larger files or communicates with the serving device for a longer period of time. As wireless broadcast medium can be used an infrared (IR) channel or a radio-frequency (RF) channel, in particular an IrDA channel, a HomeRF channel, a Bluetooth channel, a Personal Area Network (PAN) channel, an acoustic channel, or any other channel that guarantees the user a wide range of action.

[0026] For initiating the communication session and for transmitting an initial-sequence that may contain sensitive information, the unidirectional wireless communication channel can ensure that only the target device receives the initial-sequence. It is especially advantageous if a directed channel as line-of-sight link can be used, because than no other parties can eavesdrop and receive the initial-sequence. Such a channel can be an optical channel, e.g. an infrared or a laser channel, a Personal Area Network (PAN) channel, a directed radio-frequency (RF) channel, an inductive channel, a capacitive channel, or every other channel that is suitable for low-range, directed communication links.

[0027] If the serving device signalizes the reception of the sequence from the personal device, then the advantage occurs, that the user gets a feedback and knows that the serving device is ready for further communication. This can be indicated by an optical and/or acoustical signal that is given by a lamp, a LED, or a loudspeaker.

[0028] When the serving device listens periodically for the sequence from the personal device, then the advantage shows up that a sent sequence can be processed immediately.

[0029] It is very simple to set up a communication if the personal device is connected to a user, e.g. by a PAN, because the user touches then in an intuitive way the serving device for initiating the unidirectional wireless communication channel via his body. There are no additional cards or other things necessary for setting up an authenticated session .

[0030] If the response as well as the further communication over the wireless broadcast medium is protected by using a cryptosystem, than the advantage occurs, that the exchanged information is hidden perfectly and can not be uncovered by someone else. A suitable system can be a public-key cryptosystem where only the public key is exchanged once.

[0031] It is a further advantage of the invention that - in the case of a wireless unidirectional link - no direct contact between the personal and the serving device is necessary. For instance cash-cards, smart-cards, or any other card in the personal device or the personal device itself can be loaded or uploaded with information, e.g. e-mails, data, or amounts of money from a relative distance. Cards do not need to be put in devices or read devices which avoids read errors, makes PIN codes superfluously, and helps to save time.

[0032] A secure session starts right close to or in front of a serving device and can be carried on in a secure way at a larger distance. Serving devices can be installed everywhere these devices are useful, for instance: in banks, offices, warehouses, shopping centers, and outside of buildings, just to mention some examples. This brings the user more independence and freedom of action. For instance the serving device can be placed right near an advertisement for a concert. A ticket for this concert can be bought and paid already at the platform of a train station where the user is waiting and sees the advertisement for the concert. The ticket can be electronically stored on a card or the personal device and can be uploaded at the entrance of the concert. The user does not have to wait in a queue at a ticket office and will not forget to buy the ticket.

DESCRIPTION OF THE DRAWINGS

[0033] The invention is described in detail below with reference to the following schematic drawings.

FIG. 1 shows a schematic illustration of an application according to the present invention where a user wants to establish an authenticated session between his personal device and a remote serving device.

FIG. 2 shows a more detailed schematic illustration of Fig. 1.

[0034] All the figures are for the sake of clarity not shown in real dimensions, nor are the relations between the dimensions shown in a realistic scale.

DETAILED DESCRIPTION OF THE INVENTION

[0035] For the purpose of the present description the term networked pervasive computing environment is defined as an environment of both portable and fixed information devices that communicate through wireless networking technology. Communication between devices within such an environment is proximity based The startup-communication range of these devices is small. Thus, only when devices are in proximity can a session be initiated. Furthermore, establishment of communication relationships is of an ad-hoc nature. That means communication on the physical layer can take place

units of the second device 2 are connected to a second processing unit 26 that again is connected to further units for data processing or even to a network but for the sake of clarity, this is not depicted. The second transceiver 21 has a second broadcast-transmitter 22 and a second broadcast-receiver 23. Further. the second device 2 shows a signal-device 30 which is here a LED. This LED 30 is connected to the central processing unit 26. The task of the two cryptosystems 15, 25 is to encrypt and decrypt information and therewith to cover and protect the exchanged information.

[0046] To provide authenticity the present scheme employs a public-key scheme. That means a first party creates a public key by using a private key and a cryptographic algorithm and sends this public key to a second party or makes the public key available for other parties. Then. for instance the second party can encrypt information by using the received public key. The encrypted information is sent back via an insecure medium or channel, e.g. a wireless broadcast medium such as a radio-frequency (RF) channel. However, only the first party is able to decrypt the information by using their private key.

[0047] The initial-scheme according to the present invention works as follows. The user 7, for the sake of clarity not shown in Figure 2, sends from the first device 1 by using the initial-transmitter 10 the sequence 5 that comprises here an initiating token T_{init} via the unidirectional wireless communication channel 3, that is here a directed IR channel, to the second device 2. The initiating token T_{init} contains a public key K^P_{pub} of the first device 1 and a randomly chosen $nonce_P$. By transmitting the initiating token T_{init} via the unidirectional wireless communication channel 3 only the intended second device 2 can receive and respond to it. If the second device 2 receives the sequence 5 at the initial-receiver 20 and the second processing unit 26 is informed and delivered with the sequence 5, then the LED 30 is triggered by the first central processing unit 16 and signalizes the user 7 that the second device 2 is ready and a communication session can start. The session is controlled by the user at all times, which further means that the user can stop the session immediately. Normally, the second device 2 responds to the received initiating token T_{init} by sending from the second broadcast-transmitter 22 a public-key token T_{pub} as response 6 back to the first device 1 using the wireless broadcast medium 4 that is here a radio-frequency (RF). The public-key token T_{pub} that is created by the second cryptosystem 25 contains the concatenation of the public key K^S_{pub} of the second device 2 and the received $nonce_P$; the public-key token T_{pub} is encrypted using the public key K^P_{pub} of the first device 1, that was received in the initiating token T_{init}. Finally, the first device 1 receives the response 6 by the first-main receiver 12, processes this response 6 by using the first processing unit 16 and the first cryptosystem 15, and sends a communication sequence 9 that comprises a communication-parameter token T_{com} back by using the first broadcast-transmitter 13. This communication sequence 9 is also transmitted over the wireless broadcast medium 4 and is received by the second broadcast-receiver 23 of the second device 2. The communication-parameter token T_{com} is encrypted with the received public key K^S_{pub} of the second device 2.

[0048] The exchanged token can be mathematically expressed as follows.

$$T_{init} = K^P_{pub} \| nonce_P$$

$$T_{pub} = \left[K^S_{pub} \| nonce_P\right]_{K^P_{pub}}$$

$$T_{com} = |Com|_{K^S_{pub}}$$

[0049] The first cryptosystem 15 provides the initiating token T_{init} and the communication-parameter token T_{com}, whereas the second cryptosystem 25 provides the public-key token T_{pub}.

[0050] Subsequent communication between the first device 1 and second device 2 takes place over the wireless broadcast medium 4 by using the first transceiver 11 and the second transceiver 21. Thereby are used the communication parameters specified by the first device 1.

[0051] An authenticated session has been described in a first embodiment above. However, to exchange sensitive information, e.g. credit card information, authenticity alone is not sufficient. A secured, private communication link between the first device 1 and the second device 2 is required. Therefore a second embodiment is achieved by including in the communication-parameter token T_{com} a cryptographic session key K^P_{sess} generated by the first cryptosystem 15 of the first device 1. Each subsequent communication between both devices is encrypted by using this session key K^P_{sess}.

[0052] Another embodiment is addressed in relation to the first and second embodiment in the following. Typically interactions between the first device 1 that is a personal device and the second device 2 that is a serving device take place within a specific, timed context. In order to prevent the serving device 2 from being able to reuse the initiating token T_{init} over and over again, a due-date T^{init}_D is a attached to the initiating token T_{init}. Both are transmitted within the sequence 5. The personal device 1 responds to the public-key token T_{pub} only if the due-date T^{init}_D attached to the initiating token T_{init} has not yet passed. Note that the due-date T^{init}_D is relative to the personal device 1 notion of time.

[0053] Still another embodiment is a variation of the above described embodiments. Similar to the due-dated initiating token T^{init}_D, a due-date T^{sess}_D is attached to the session key K^P_{sess} generated by the personal or first device 1 and transmitted over the wireless broadcast me-

is connected to a user (7), and wherein said user (7) touches said remote second device (2) for initiating said unidirectional wireless communication channel (3) via the user's body.

13. The method of claim 1, wherein one of said two devices (1, 2) sends at least a communication parameter and/or a session key.

14. The method of claim 1, wherein said response (6) over said wireless broadcast medium (5) is protected by using a cryptosystem, preferably a public-key cryptosystem.

15. The method of claim 1, wherein said encryption information comprises a password and/or a public key.

16. An apparatus for providing an authenticated communication session with at least one remote device (2), comprising

- an initial-transmitter (10) for transmitting a sequence (5) via a unidirectional wireless communication channel (3) to said remote device (2),
- a receiver (12) for receiving encrypted information from said remote device (2) via a wireless broadcast medium (4), and
- a cryptographic system (15) providing encryption information which is transmitable over said unidirectional wireless communication (3) channel to said remote device (2) and whereby said receiver (12) is able to receive over said wireless broadcast medium (4) encrypted information which is processable by said cryptographic system (15).

17. An apparatus for providing an authenticated communication session with at least one device (1), comprising

- an initial-receiver (20) for receiving a sequence (5) via a unidirectional wireless communication channel (3) from said device (1) in order to obtain encryption information,
- a cryptographic system (25) for processing said encryption information, and
- a transmitter (22) for transmitting encrypted information to said device (1) over a wireless broadcast medium (4).

18. A communication system for providing an authenticated communication session of a first device (1) with a second device (2), each having a cryptographic system (15, 25) for encoding and decoding of information, whereby

- said first device (1) comprises an initial-transmitter (10) for sending a sequence (5) via a unidirectional wireless communication channel (3) to said second device (2) in order to furnish said second device (2) with encryption information, and a first transceiver (11) for encrypted communication between said first and second device (1, 2) over a wireless broadcast medium (4), and
- said second device (2) comprises an initial-receiver (20) for receiving said sequence (5) from said first device (1) via said unidirectional wireless communication channel (3) in order to obtain said encryption information, and a second transceiver (21) for encrypted communication between said first and second device (1, 2) over said wireless broadcast medium (4).

19. The apparatus according to claim 16, further comprising a transmitter (13) which is able to transmit encrypted information over said wireless broadcast medium (4).

20. The apparatus according to claim 16, whereby said initial-transmitter (10) transmits said sequence (5) via said unidirectional wireless communication channel (3) in a reach of a few meters.

21. The apparatus according to claim 16 or 17, whereby said wireless broadcast medium (4) is an optical channel, an acoustic channel, a radio-frequency (RF) channel, a HomeRF channel, a Bluetooth channel, or a Personal Area Network (PAN) channel.

22. The apparatus according to claim 16 or 17, whereby said wireless broadcast medium (4) has the same reach or a reach beyond the reach of said unidirectional wireless communication channel (3).

23. The apparatus according to claim 17, further comprising a signal-device (30) for signalizing the reception of said sequence (5), preferably by an optical and/or acoustical device such as a LED and/or a loudspeaker.

24. The apparatus according to claim 17, whereby said initial-receiver (20) listens periodically for said sequence (5).

25. The communication system according to claim 18, whereby one of said two devices (1, 2) is able to send a communication parameter and/or a session

Fig. 1

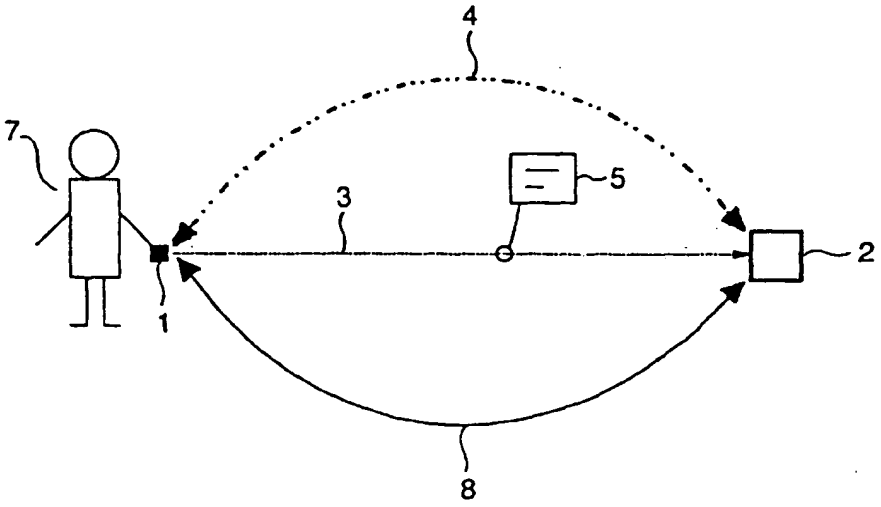
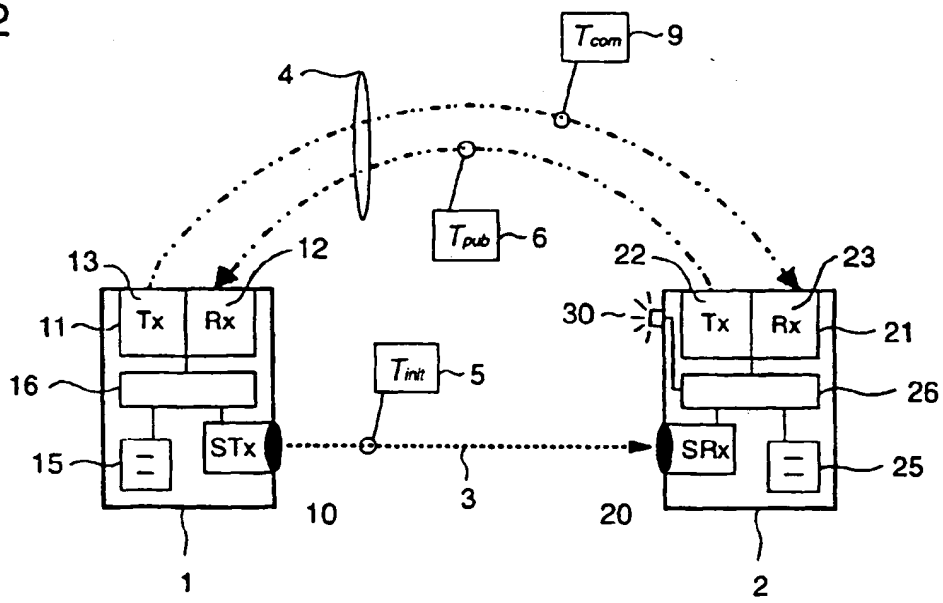


Fig. 2



ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 10 1457

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

09-06-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0756397 A	29-01-1997	JP 9167098 A	24-06-1997
		US 5887063 A	23-03-1999
EP 0843425 A	20-05-1998	US 5796827 A	18-08-1998
		CN 1185065 A	17-06-1998
		JP 10228524 A	25-08-1998
GB 2254225 A	30-09-1992	US 5500888 A	19-03-1996

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82